4Ш

УДК 681.31

Б.М. Шевчук
Інститут кібернетики імені В.М. Глушкова НАН України
Україна, 03680, м. Київ, проспект Академіка Глушкова, 40

Надійна і захищена передача інформації в радіомережах промислового призначення та для зв'язку між мобільними роботами і рухомими системами

B.M. Shevchuk
V.M. Glushkov Institute of Cybernetic of NAS of Ukraine
Ukraine, 03680, Kiev, Glushkova ave., 40

Reliable and Protected Data Transmission in Radio Networks for Industrial Use and for Communication between Mobile Robots and Mobile Systems

Б.М. Шевчук
Институт кибернетики имени В.М. Глушкова НАН Украины
Украина, 03680, г. Киев, проспект Академика Глушкова, 40

Надежная и защищенная передача информации в радиосетях промышленного назначения и для связи между мобильными роботами и двигательными системами

У статті запропоновані адаптивні методи надійної та захищеної передачі інформації в сенсорних і локально-регіональних радіомережах з самоорганізацією передачі пакетів інформації. Надійна та захищена передача інформації в таких мережах ґрунтується на можливості формування альтернативних шляхів ретрансляції пакетів між сусідніми абонентськими системами радіомережі, на основі адаптивного вибору бази канальних сигналів для підтримки абонентами необхідного енергетичного співвідношення сигнал/шум в радіоканалі, а також досягається за рахунок комплексного кодування та шифрування даних, що підлягають передачі, включаючи адаптивне компактне кодування суттєвих відліків сигналів (відеосигналів), компактне кодування двійкових послідовностей, шифрування пакетів даних з одноразовим шифром, завадостійке кодування компактних і криптостійких даних пакетів з використанням кодів поля Галуа та шляхом формування відповідних інтервально-імпульсних шумоподібних сигналів, прихованих в шумах радіоканалу.
Ключові слова: сенсорні та локально-регіональні радіомережі, самоорганізація передачі пакетів інформації, методи захищеної та надійної передачі інформації.

The article suggested the adaptive methods of reliable and protected data transmission in sensor and local radio networks with data packet selftransfer. Reliable and protected data transmission in such networks is based on the possibility of creating alternative ways of relaying packets between neighboring subscriber systems of radio network based on adaptive selection of the base channel signals to support necessary energy signal / noise ratio in the radio channel by subscribers, and is achieved by integrated coding and encryption data to be transferred, including adaptive compact coding of significant signal samples (video), compact binary coding sequences, encryption of data packets from one-time code, antinoise coding and compact crypto resistant data packets with codes and Galois fields by forming the corresponding interval-pulse noise-like signals hidden in radio noises. To relay compact, crypto resistant and noise immune packets of information over long distance, the callers use directed antenna systems and provide adaptive selection of encoding methods and the formation of noise-like signal-code sequences.
Key words: sensor and local radio networks, data packet selftransfer, methods of reliable and protected data transmission

В статье предложены адаптивные методы надёжной и защищенной передачи информации в сенсорных и локально-региональных радиосетях с самоорганизацией передачи пакетов информации. Надёжная и защищенная передача информации в таких сетях базируется на возможности формирования альтернативных путей ретрансляции пакетов между соседними абонентскими системами радиосети, на основе адаптивного выбора базы канальных сигналов для поддержки абонентами необходимого энергетического соотношения сигнал/шум в радиоканале, а также достигается за счет комплексного кодирования и шифрования данных, подлежащих передаче, включая адаптивное компактное кодирование существенных отсчетов сигналов (видеосигналов), компактное кодирование двоичных последовательностей, шифрование пакетов данных с одноразовым шифром, помехоустойчивое кодирование компактных и криптостойких данных пакетов с применением кодов поля Галуа, а также путем формирования соответствующих интервально-импульсных шумоподобных сигналов, скрытых в шумах радиоканала.
Ключевые слова: сенсорные и локально-региональные радиосети, самоорганизация передачи пакетов информации, методы защищенной и надежной передачи информации.

Вступ

Для передачі інформації від рухомих та літаючих об’єктів і систем, віддалених промислових об’єктів моніторингу безальтернативним способом зв’язку є використання комп’ютерних радіомереж (сенсорних, локально-регіональних, глобальних (супутникових, мікросупутникових)). Застосування лазерних, інфрачервоних та ультразвукових систем зв’язку характеризується вузькою прикладною направленістю і в більшості випадків не замінює радіопередачу даних. Суттєвим недоліком радіомереж є той факт, що в процесі передачі пакетів інформації між віддаленими абонентами інформація може бути перехоплена несанкціонованими абонентами, а при наявності потужних електромагнітних завад та імпульсних випромінювань передача і прийом інформації стає неможливою. Вкрай негативні випадки застосування радіомереж – можливість перешкодження передачі інформації спеціалізованими передавачами, а також передача хибної (неправдивої) інформації несанкціонованими абонентами-імітаторами.

В промисловості випуск конкурентоспроможних товарів, систем та засобів не можливий без впровадження нових технологій та розгалужених комп’ютерних мереж моніторингу якості виробництва, включаючи моніторинг якості виконання технологічних процесів, результатів випробувань, вимірювання параметрів деталей вузлів та виробів. Неперервно-періодичному контролю підлягають параметри матеріалів і вироби постачальників, вимірювальні дані (показники вимірювальних приладів) та фрагменти діагностичних сигналів, які характеризують якість виконання відповідної технологічної операції. Контролю також підлягають фіксовані і рухомі відеодані процесів реалізації окремих технологічних операцій, зображення фрагментів виробів, екологічні показники виробничих ділянок, цехів та підприємства в цілому. В результаті реалізації комплексу заходів з моніторингу якості виробництва, кожний виріб або партія виробів супроводжується записами даних в центральному сервері підприємства, які підтверджують високу кількість виробів. Враховуючи високі електромагнітні випромінювання, імпульсні завади та завади від силового електрообладнання у виробничих цехах, актуальною проблемою при організації оперативного збору, обробки і передачі моніторингової інформації є побудова надійних та захищених комп’ютерних радіомереж моніторингу якості виробництва в тяжкій промисловості, в металургії, у ливарному виробництві, в авіабудуванні, в будівництві та сільському господарстві.

В процесі організації передачі інформації (відеоданих, сигналів, масивів даних) між мобільними роботами і рухомими системами виникають ті ж самі задачі, пов’язані з реалізацією надійного та захищеного радіозв’язку. Оскільки передача інформації між рухомими системами здійснюється невеликими порціями (пакетами інформації), то актуальною проблемою є оптимізація процесів оброблення, кодування та передавання пакетів інформації з урахуванням мінімізації кількості успішних передач пакетів в ме-

режі, зменшення їх тривалості передавання при досягненні необхідного ступеня криптозахисту даних та захисту їх від спотворень природними, промисловими та штучними завадами.

Метою даної статті є розробка методів та алгоритмів ефективної адаптивної обробки, кодування даних та передачі пакетів інформації в умовах дії потужних канальних завад. Враховуючи тенденції розвитку радіомереж, включаючи широке застосування mesh-мереж, формування компактних та захищених пакетів кожною абонентською системою призводить до суттєвого підвищення ефективності використання спільного ресурсу мережі – радіоканалу.

Методологічні та алгоритмічні основи реалізації надійної та захищеної передачі інформації в радіомережах

В радіомережах з урахуванням наявних канальних ресурсів (робочої смуги частот F, кількості частот L_f, кодових L_k та просторових L_p моноканалів) передача інформації здійснюється нетривалими пакетами, довжина (величина) яких, переважно, є змінною і вимірюється сотнями-тисячами бітів. Ефективність роботи радіомережі характеризується поточною максимальною швидкістю передачі інформаційних пакетів (ІП) $R_{\max i}$, величина яких суттєво залежить від якісних і системних показників канальних ресурсів (величин F, $L_\Sigma = L_f + L_k + L_p$, енергетичного співвідношення сигнал/шум в моноканалах) та параметрів адаптивної обробки, кодування і передачі даних, тобто $R_{\max} = f(F, L_\Sigma, P_n, (E_b / J_o)_H, 1/B, K_{cm})$, де P_n – ймовірність помилкового прийому елементарного дискретного сигналу або кодової послідовності, $(E_b / J_o)_n$ – необхідне енергетичне співвідношення сигнал/шум в моноканалі, $E_b = P_c \cdot T_b$, P_c – потужність сигналу, T_b – тривалість бітової або кодової послідовності, $J_o = J / F$, J – середня потужність сумарних завад у каналі зв'язку (в точці прийому інформації), $B = F \cdot T_b$ – база канального сигналу, K_{cm} – сумарний коефіцієнт стиску даних, включаючи стиск даних до формування ІП (стиск з допустимими втратами сигналів (відеосигналів) та стиск бітових послідовностей без втрат), а також стиск даних в процесі формування та передачі ІП.

Таким чином, основою для надійної та ефективної передачі даних у радіомережах є підтримка абонентами мережі необхідного енергетичного співвідношення $(E_b / J_o)_n$ в радіомережі [1], компактного кодування даних, що підлягають передачі, комплексного завадостійкого кодування компактних і криптостійких даних шляхом поєднання рекурсивного кодування послідовностей бітів ІП з використанням кодів поля Галуа [2] та формуванням відповідних інтервально-імпульсних шумоподібних сигналів [3]. В результаті дані ІП передаються в шумах радіоканалу, а за рахунок попереднього вибору мінімально необхідної бази шумоподібних сигналів (ШПС) забезпечуються умови надійного прийому бітових або кодових послідовностей ІП. У випадку враження завадами інформативного ШПС виправлення помилок прийому даних досягається шляхом рекурентного визначення місцезнаходження того символу, який потребує виправлення. Одним із ефективних способів реалізації надійної передачі пакетів інформації є побудова коміркових мереж (рис. 1) з самоорганізацією передачі пакетів даних [4], [5], при цьому комірки об'єднуються в кластери, в яких одна із АС виконує функції «вершини» кластера і забезпечує підвищену дальність зв'язку з «вершинами» сусідніх кластерів.

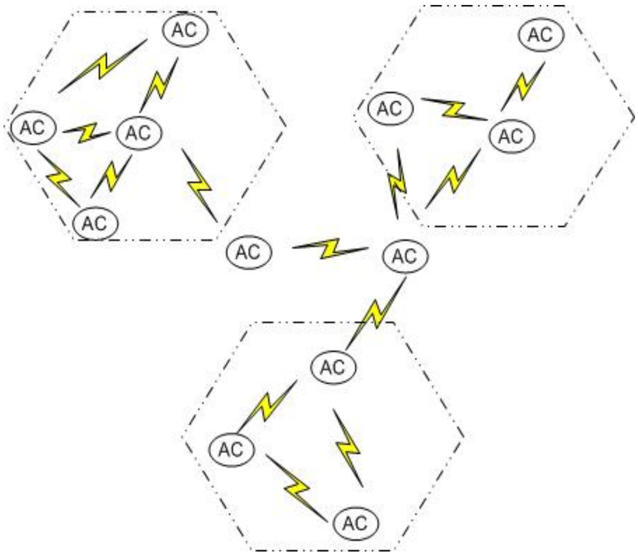


Рисунок 1 – Структура багатокластерної коміркової радіомережі

За рахунок цього забезпечується покриття зв'язком великої кількості віддалених АС на заданій території. В коміркових радіомережах надійність зв'язку досягається за рахунок утворення різноманітних резервних шляхів передачі ІП між сусідніми АС. При цьому кожна АС відслідковує якість каналу зв'язку з сусідніми АС, визначаючи та запам'ятовуючи поточні параметри енергетичного співвідношення сигнал/шум в каналі зв'язку. На основі отриманих даних роутерами (АС-ретранслятори) комірок і кластерів формують таблиці маршрутизації при передачі ІП між віддаленими абонентами багатокластерної радіомережі. Одним із ефективних способів побудови протоколів маршрутизації ІП між віддаленими АС багатокоміркових мереж є врахування комплексу поточних параметрів про стан проміжних каналів зв'язку між сусідніми абонентами всієї ланки ретрансляції ІП та показників відхилення від оптимального (мінімального) шляху ретрансляції пакетів. Для підвищення надійності передачі інформації при прийнятті рішення ретрансляції даних в режимі «від сусіда до сусіда» доцільно в напрямку оптимального шляху визначати резервні ланки ретрансляції інформації. Таким чином, в залежності від відстані між віддаленими абонентами, що забезпечують передачу / прийом ІП, маршрутизація пакетів здійснюється на рівні комірки, багатьох комірок (кластеру), багатьох кластерів. Реалізація комплексу алгоритмів компактного кодування, криптостійкого шифрування та завадостійкого кодування даних у місцях утворення інформаційних потоків та формування ІП засобами АС суттєво зменшує кількість пакетів, які ретранслюються проміжними абонентами, що визначаються в процесі передачі інформації між віддаленими абонентами багатокластерної коміркової радіомережі. Основою для зменшення кількості пакетів та їх тривалості, які з високою ймовірністю успішно ретранслюватимуться «від сусідньої АС до сусідньої АС» є реалізація абонентами мережі адаптивних алгоритмів компактного кодування первинних даних, шифрування та передачі інформації.

Ефективне функціонування АС коміркових мереж здійснюється в режимі передачі інформації «кожний з кожним» та періодичної підтримки зв'язку з сусідніми абонентами з урахуванням вибору основного та альтернативних шляхів передачі ІП. Передача інформації здійснюється в три етапи: встановлення зв'язку між парою (парами) абонентів радіомережі; передача заявленої кількості пакетів; завершення передачі пакетів. Останній етап передачі інформації може бути упущеним після успішної передачі всіх ІП. В залежності від продуктивності абонентського обладнання передача ІП може здійснюватись по єдиному радіоканалу (моноканалу), по одному із декількох вільних радіоканалів або по відповідній кількості вільних радіоканалів.

Також можлива передача бітових послідовностей ІП паралельно по декількох каналам (частотним, кодовим). Передача ІП між абонентами радіомережі може здійснюватись в режимах централізованого управління передачею даних та на основі множинного доступу конфліктуючих абонентів до спільного ресурсу мережі – радіоканалу. В режимі централізованої передачі інформації центральна станція мережі (комірки, кластера) в широкомовному режимі передає керуючий пакет-квитанцію (КПК), в якому повідомляє про адресу активного абонента. Останній, отримавши КПК, передає ЦС ІП, а всі інші абоненти мережі перебувають в режимі очікування. В КПК ЦС призначає базу та типи сигнально-кодових послідовностей ІП. Доцільність використання режиму централізованої передачі інформації виникає у випадку активізації значної кількості абонентів (більше 60 – 70% від загальної кількості), які прагнуть передати ІП. В режимі множинного доступу до спільних ресурсів (рис. 2) абоненти прослуховують радіоканал і у випадку його зайнятості відкладають спробу передачі ІП на випадковий інтервал часу. У випадку виявлення вільного стану радіоканалу та успішної реалізації процедури множинного доступу один із активних абонентів формує і передає відповідному абоненту-адресату пакет-запит (П-З) з тестовими сигнально-кодовими послідовностям з різною базою, наприклад, з мінімальною $B_{\min}$, середньою B та максимальною $B_{\max}$. Абонент-адресат, проаналізувавши якість прийому двійкових повідомлень П-З, передає абоненту- відправнику П-З зворотній пакет, в якому повідомляє про вибір мінімально-необхідної бази ШПС із набору сигнально-кодових послідовностей для успішної передачі ІП. При цьому адаптивно підбирається тривалість елементарного символу та кількість елементів ШПС.

При передачі вимірювальних сигналів, зображень, мультимедійних даних для формування компактних ІП здійснюється фільтрація сигналів (відеосигналів), пошук і компактне кодування амплітудно-часових параметрів найбільш інформативних (суттєвих) відліків згинаючої сигналів. Структура алгоритму компактного кодування сигналів (відеосигналів) наведена на рис. 3.

Для мінімізації інформаційних потоків і виконання обчислювальних операцій засобами АС, резервування часу для обробки і кодування даних інтервал-опиту (дискретизації) сигналів вибирають адаптивним з урахуванням залежності $t_{\partial i} = f(f_{\max}, \Delta X_i^F, \delta_{вх})$, де $f_{\max}$–максимальна інформативна частота спектра сигналу, $\Delta X_i^F = X_i^F - X_{i-1}^F$ – поточний приріст відфільтрованого сигналу, X_i^F – поточний відлік відфільтрованого сигналу, $\delta_{вхi} = \Delta X_i^N = |X_{CBi} - X_{вхi}|$ – поточна оцінка величини вхідного співвідношення сигнал / шум в околиці суттєвого відліку (СВ). Після реалізації оперативної фільтрації на відфільтрованій кривій здійснюється пошук амплітудно-часових характеристик суттєвих відліків-екстремумів (СВ-Е) та відповідних їм показників $\delta_{вхi}$. Вважаємо, що параметри екстремумів визначені приблизно (грубо) і при значних шумах (коли вхідні шуми в околиці СВ перевищують допустиму величину, тобто коли $\delta_{вхi} > \delta_{доп}$) параметри СВ-$Е_{гр}$ з практичної точки зору в повній мірі відтворюють візуальні характеристики огинаючої сигналу (відеосигналу). При наявності чистих від шумів ділянок сигналу (коли $\delta_{вх} \le \delta_{доп}$) здійснюється уточнене визначення параметрів СВ-$Е_т$ та проміжних суттєвих відліків-точок перегину (ВС-$ТП_т$). В процесі компактного різницевого кодування СВ-$Е_{гр}$ кодуються з використанням мінімальної кількості біт $Q_{\min}$, а СВ-$Е_т$ і СВ-$ТП_т$ кодуються з використанням максимальної кількості біт $Q_{\max}$.

Після компактного кодування сигналів з допустимими втратами масиви даних підлягають компактному кодуванню без втрат, криптозахисту та завадостійкому ко-

дуванню. При цьому кожна АС мережі володіє закритим ключем (довгим числом), з використанням яких пари абонентів (приймач і передавач ІП) формують одноразові шифри для криптозахисту даних ІП. В результаті на АС формуються стислі та захищені масиви даних [6], які є псевдохаотичними беззбитковими двійковими послідовностями, і які, при формуванні ІП з урахуванням поточного співвідношення сигнал/шум в радіоканалі, перетворюються у послідовності хаотичних шумоподібних інтервально-імпульсних сигналів.

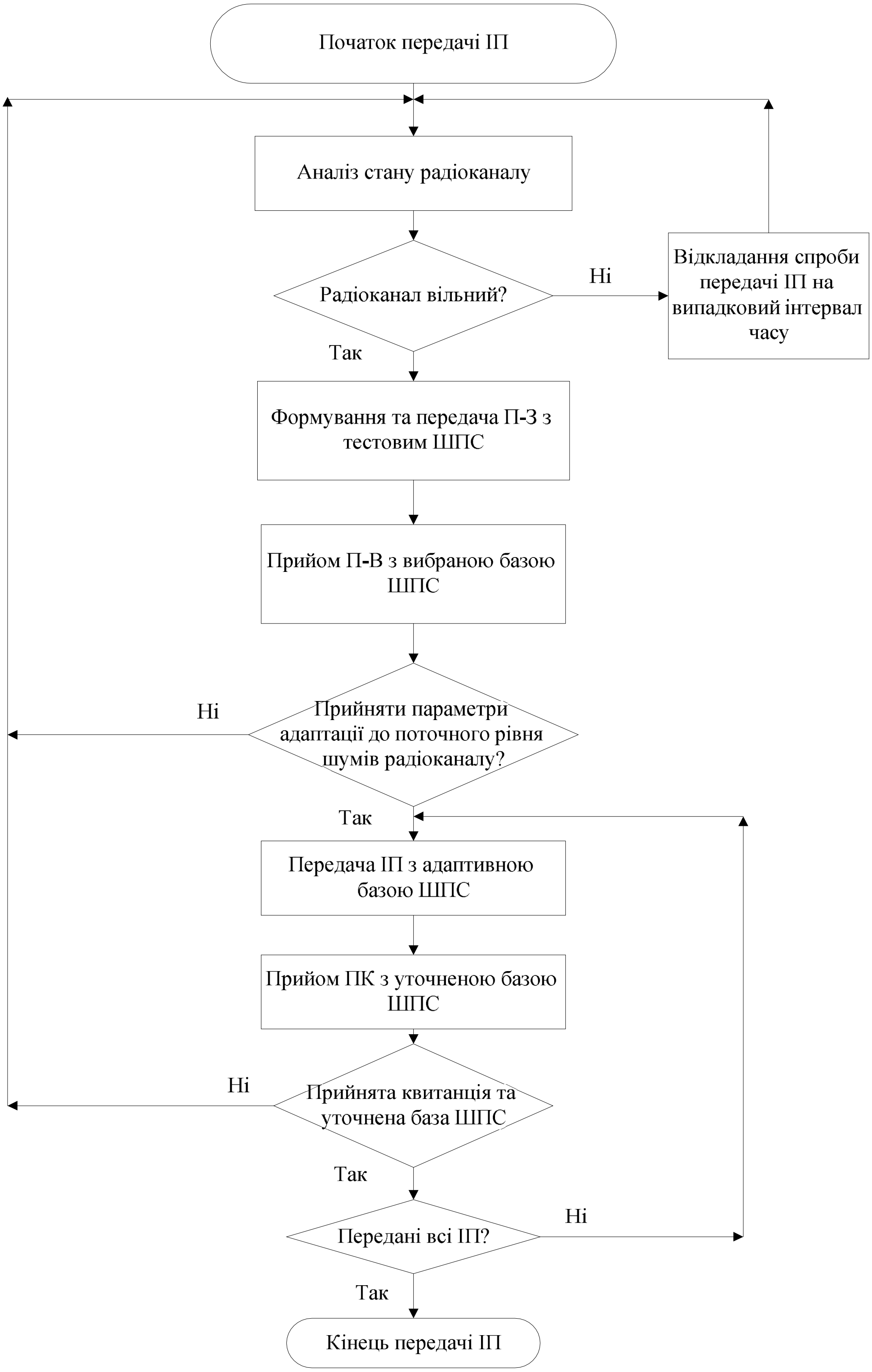


Рисунок 2 – Структура алгоритму адаптивної передачі ІП в режимі множинного доступу абонентів до радіоканалу

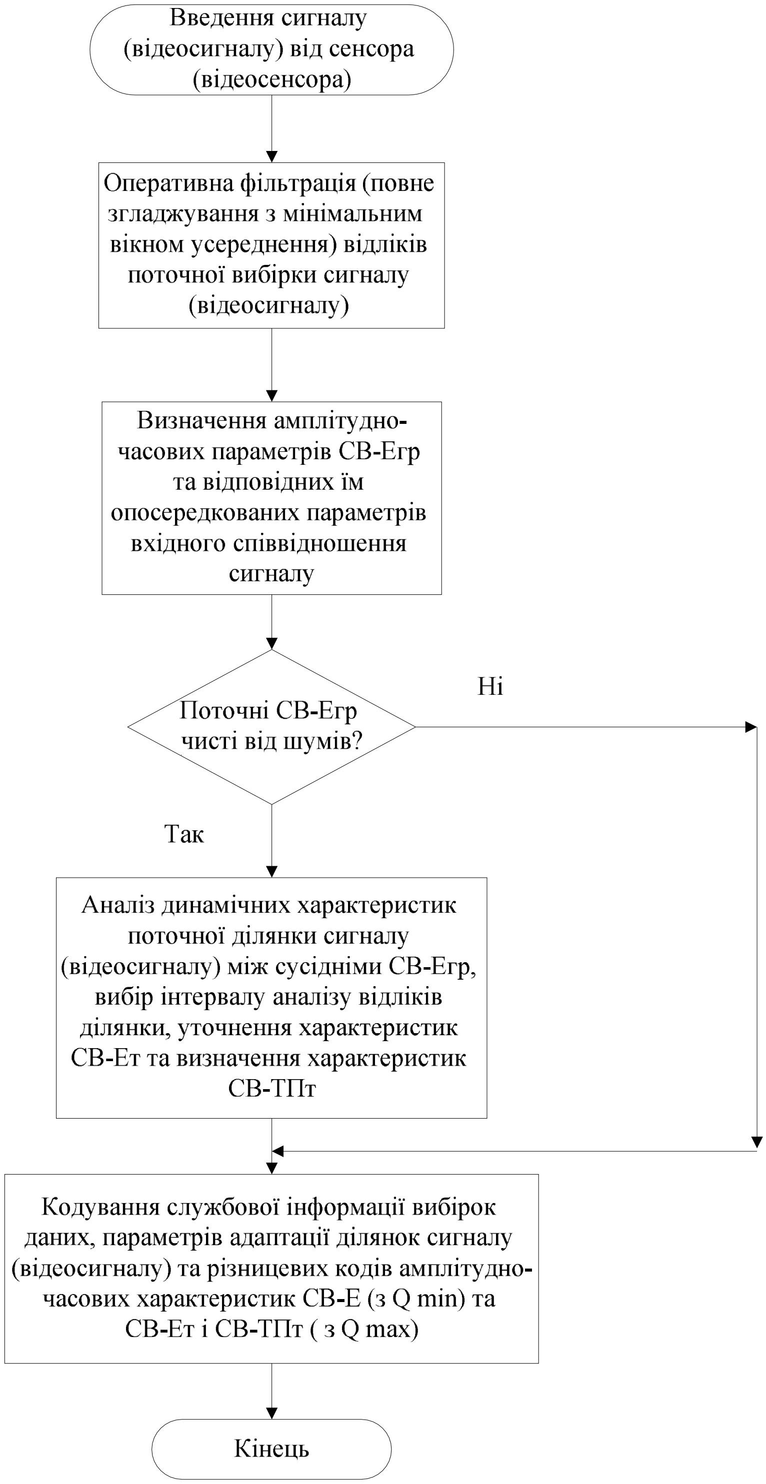


Рисунок 3 – Структура алгоритму компактного кодування сигналів (відеосигналів)

Висновки

Основою для надійної і захищеної передачі ІП в радіомережах є використання протоколів передачі інформації з самоорганізацією ретрансляції пакетів між сусідніми абонентами коміркових радіомереж, які формують альтернативні шляхи передачі криптостійких та завадостійких пакетів, а також адаптивний вибір бази шумоподібних сигналів пакетів. З метою зменшення кількості пакетів, що підлягають передачі в спільному радіоканалі, на кожній абонентській станції забезпечується визначення та компактне кодування найбільш інформативних відліків сигналів (відеосигналів), компактне кодування масивів без втрат, крипостійке та завадостійке кодування даних пакетів. Для ретранс-

ляції компактних, криптостійких та завадостійких пакетів інформації на великі відстані між абонентами доцільно використовувати направлені антенні системи та забезпечувати адаптивний вибір методів кодування і формування шумоподібних сигнально-кодових послідовностей. Подальшим перспективним напрямком підвищення ефективності функціонування мереж є передача заявлених масивів даних між сусідніми абонентами одним компактним та псевдохаотичним пакетом.

Література

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Скляр Б. ; [пер. с анг.]. – М. : Издательский дом «Вильямс», 2003. – 2-е изд. – 1104 с.
2. Николайчук Я.М. Спосіб передавання та приймання інформації / Я.М. Николайчук, Т.М. Гринчишин, А.Р. Воронич. – Патент України № 96853, H03M 13/00. – Бюл. № 23, 2011. – 6 с.
3. Технологія багатофункціональної обробки і передачі інформації в моніторингових мережах / [Шевчук Б.М., Задірака В.К., Гнатів Л.О., Фраєр С.В.]. – К. : Наук. думка, 2010. – 370 с.
4. Гейер Д. Беспроводные сети. Первый шаг / Гейер Д. ; [пер. с анг.]. – М. : Издательский дом «Вільямс», 2005. – 192 с.
5. Shelby Z. 6LoWPAN: TheWireless Embedded Internet / Z. Shelby, C. Bormann. – WILEY, 2009. – 223 p.
6. Шевчук Б.М. Підвищення ефективності передачі пакетів інформації в сенсорних та локально-регіональних радіомережах для організації зв'язку між мобільними роботами і рухомими системами / Б.М. Шевчук // Штучний інтелект. – 2011. – № 3. – С. 417-422.

Literatura

1. Skljar B. Cifrovaja svjaz'. Teoreticheskie osnovy i prakticheskoe primenenie, 2-e izd.: per. s ang. M.: Izdatel'skij dom "Vil'jams". 2003. 1104 s.
2. Nikolajchuk Ja.M. Sposib peredavannja ta pryjmannja informacii. Patent Ukriny № 96853, H03M 13/00. Bjul. № 23. 2011. 6 s.
3. Shevchuk B.M. Tehnologija bagatofunkcional'noi obrobky i peredachi informacii v monitoringovyh merezhah. K.: Nauk. dumka. 2010. 370 s.
4. Gejer D. Besprovodnye seti. Pervyj shag: Per. s ang. M.: Izdatel'skij dom "Vil'jams". 2005. 192 s.
5. Shelby Z. 6LoWPAN: TheWireless Embedded Internet. WILEY. 2009. 223 p.
6. Shevchuk B.M. Shtuchnyj intelekt. 2011. № 3. S. 417-422.

B.M. Shevchuk

Reliable and Protected Data Transmission in Radio Networks for Industrial Use and for Communication between Mobile Robots and Mobile Systems

The article suggested the adaptive methods of reliable and protected data transmission in sensor and local radio networks with data packet selftransfer. Reliable and protected data transmission in such networks is based on the possibility of creating alternative ways of relaying packets between neighboring subscriber systems of radio network based on adaptive selection of the base channel signals to support necessary energy signal / noise ratio in the radio channel by subscribers, and is achieved by integrated coding and encryption data to be transferred, including adaptive compact coding of significant signal samples (video), compact binary coding sequences, encryption of data packets from one-time code, antinoise coding and compact crypto resistant data packets with codes and Galois fields by forming the corresponding interval-pulse noise-like signals hidden in radio noises. To relay compact, crypto resistant and noise immune packets of information over long distance, the callers use directed antenna systems and provide adaptive selection of encoding methods and the formation of noise-like signal-code sequences.

Стаття надійшла до редакції 07.05.2012.